REMARKS/ARGUMENTS

These remarks are responsive to the non-final Office Action dated February 6, 2008. Applicants respectfully request entry of this Amendment. Claims 46, 49, 50, 62 and 63 have been amended and claims 64 and 65 have been added. No new matter has been added. Claims 1, 4-6, 11, 32-34, 40-50, 53-54, and 56-65 are pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Claim Rejections Under 35 U.S.C. §103(a)

Claims 1, 4, 32-34, 40-50, 53, 56, 58 and 60-62 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fink *et al.* (U.S. Patent No. 6,496,936) and Makinson *et al.* (U.S. Patent No. 7,023,861). This rejection is respectfully traversed.

Claim 1 recites, *inter alia*, "a firewall configured to: receive data packets over a first network; classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus; forward the data packets of the first type to a destination without testing by a virus scanning engine; and forward the data packets of the second type to a virus scanning engine for testing." Contrary to the Office Action's assertions, neither Fink nor Makinson, either separately or in combination, teaches or suggests such features. The Office Action concedes, at p. 3, that Fink does not teach or suggest packets of a first type which cannot contain a virus and packets of a second type which can contain a virus. Instead, the Office Action relies on Makinson. Specifically, the Office Action cites col. 6, ll. 18-24 and col. 2, ll. 50-52 of Makinson as allegedly teaching the first and second types of packets recited in claim 1. Applicants respectfully disagree.

Although Makinson describes using a data packet analyzer that can be responsive to different properties of data packets to determine whether or not they are to be passed to the malware scanner, Makinson describes making such a determination based on whether the malware scanner is able to deal with the network layer protocol of the packet. Col. 4, ll. 45-47 (stating "[i]t may well be that the malware scanner 16 is only able to deal with network layer protocols of particular types…"). Thus, Makinson describes determining whether to pass a packet to a malware scanner or not based on the capability of the scanner and not whether the

packets can, or cannot, contain a virus as recited in claim 1. Indeed, Makinson describes sending all packets of a supported porotocol to the scanner, regardless of whether the packet can or cannot contain a virus. Col. 4, ll. 42-65. Accordingly, claim 1 is allowable for at least these reasons.

Additionally, claim 1 recites that the firewall is configured to perform the classifying function. Significantly, nowhere does Fink or Makinson teach or suggest that a firewall performs such classification. Indeed, Makinson does not even discuss firewalls. Fink, on the other hand, describes that the pre-filtering module and the firewall could be implemented as a combined device (i.e., a black box), Fink does not teach or suggest that the firewall performs the classification function. Stated differently, the pre-filtering module and the firewall could be implemented as separate components of a combined device (i.e., the pre-filtering module may still operate independently of and/or separately from the firewall). In fact, one of the stated goals of Fink is to relieve a firewall of large computational burdens by using pre-filtering module 30 to receive packets ***before*** the firewall. Based on the foregoing, not only does Fink fail to teach or suggest a firewall configured to perform the classification recited in claim 1, Fink also clearly teaches away from such features. Accordingly, claim 1 is allowable for this additional reason.

Amended independent claims 49, 50 and 62 all relate to, *inter alia*, classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus. As discussed above, Fink describes using a pre-filtering module including a classification engine, wherein the engine analyzes a portion of information in a packet and determines whether the packet is permitted. Col. 8, ll. 39-43. Makinson, on the other hand, describes a data packet analyzer responsive to different properties of data packets to determine whether or not they are to be passed to the malware scanner. Col. 2, ll. 50-52. However, neither of these descriptions, either separately or in combination, teaches or suggests classifying data packets into a first type which ***cannot contain a virus*** and packets of a second type which can contain a virus. In other words, there is no teaching or suggestion in either Fink or Makinson of considering whether a data packet is of a packet type that can or cannot contain a virus. Accordingly, claims 49, 50 and 62 are allowable for at least these reasons.

Claims 4, 32-34, 40-48, 53, 56, 58, 60 and 61 are dependent claims and are thus allowable for at least the same reasons as their base independent claims and further in view of the novel and non-obvious features recited therein. For example, claim 4 recites, "wherein the classifying comprises determining that data packets of the first type contain real time data." The Office Action asserts, at p. 7, that Makinson describes such a feature at col. 6, ll. 18-24. However, the cited passage merely relates to using one type of scanner (i.e., a software based scanner) to perform non-time critical scanning while using another type of scanner (i.e., an optional high performance hardware scanner) for other scanning. Col. 6, ll. 18-24. Even assuming, without conceding, that time critical data constitutes real time data, Makinson still does not teach or suggest that the classification of packets between a first type which cannot contain a virus and a second type which can contain a virus is based on determining whether the packets require non-time critical scanning or not. Fink does not cure these deficiencies of Makinson. Accordingly, claim 4 is allowable for this additional reason.

Claims 5, 57, 59 and 63 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fink in view of Makinson and Lee (U.S. Patent No. 7,047,561, "Lee"). Claims 6 and 54 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fink in view of Makinson and Lyle (U.S. Patent No. 6,886,102, "Lyle"). Claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Fink in view of Makinson and Franczek *et al.* (U.S. Patent No. 6,397,335, "Franczek"). Applicants respectfully traverse these rejections.

Claims 5, 11, 54, 57, 59 and 63 are dependent claims and thus incorporate each and every feature of their base independent claims. As discussed above, neither Fink nor Makinson teaches or suggests each and every feature of claims 1, 49, 50 and 62. Lee, Lyle and Franczek do not cure these deficiencies of Fink and Makinson. Accordingly, notwithstanding whether the asserted combinations are valid, the combinations would not have resulted in the features as recited in claims 1, 49, 50 and 62. Moreover, claims 5, 11, 54, 57, 59 and 53 are allowable for at least the same reasons as their base independent claims and further in view of the novel and non-obvious features recited therein.

For example, claims 5, 57, 59 and 63 relate to wherein classifying the data packets based on the contents of the data packets includes determining whether at least one of the data packets

includes content for a real-time audio or video data stream. Contrary to the Office Action's assertions, none of the cited references, either separately or in combination, teaches or suggests such features. In the Office Action's rejection of the aforementioned claims, the Office Action cites passages of Lee relating to data packets for multi-media. Office Action, p. 11; Lee, Col. 1, ll. 58-62; col. 4, ll. 36-39. Even assuming, without conceding, that Lee describes data packets for multi-media, the cited references still lack a teaching or suggestion of classifying data packets by determining whether the data packets includes content for real-time audio or video data streams.

Further, the Office Action's alleged motivation for making the asserted combination is that one of ordinary skill would want to have a firewall used in association with real-time Internet application. Not only does the Office Action's alleged motivation not address why one would classify data packets by determining whether the data packets include content for real-time audio or video streams, the Office Action is merely applying impermissible hindsight reconstruction to piece together the prior art references using Applicants' Specification as a blueprint. Accordingly, claims 5, 57, 59 and 63 are allowable for this additional reason.

CONCLUSION

Based on the foregoing, Applicants respectfully submit that the application is in condition for allowance and a Notice to that effect is earnestly solicited. Should the Examiner believe that anything further is desirable in order to place the application in even better form for allowance, the Examiner is respectfully urged to contact Applicants' undersigned representative at the below-listed number.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated this 28th day of May, 2008

By: /Chunhsi Andy Mu/
Chunhsi Andy Mu, Reg. No. 58,216

1100 13th St. N.W.
Washington, D.C. 20005-4051
Tel: (202) 824-3000